INTERNET VIRUS

Mrs. BLACKBURN. Madam President, it has been so wonderful to be in Tennessee over the past couple of weeks and to have the opportunity to listen to Tennesseans. We have listened and talked to local elected officials and teachers and parents from one corner of the State to another. They are very aware and are truly focused on the challenges we are going to be facing this fall in just a few weeks.

Some of our school systems in Tennessee are going to be going back to school the first week of August. They have a lot of questions as to whether they are going to end up with classes meeting in person or online.

Up until now, students have relied on virtual schooling platforms to stay connected to their teachers, and it is likely that in many communities, this system will continue at least through the fall semester.

Relying on Google and other educational software providers keeps teachers and families safe from COVID–19, but these programs come with their own brand of hazards. Our increased reliance on Big Tech has highlighted just how vulnerable we are when things go awry. Even the platforms that have become commonplace over the years pose risks and not only just risks to children. You need look no further than last week's Twitter meltdown for evidence of how quickly a hacker or even an insider can turn a few tweets into a threat.

I will tell you this: In Tennessee, we have a lot of security moms. Those security moms you hear so much about are really back in full force. They are concerned. They are paying close attention, and they are not going to back off of the Googles and the Facebooks and the Instagrams. They want to see these companies held accountable and transparent about how they follow and use data because when they see their children spending hours staring at TikTok or YouTube, they are beginning to see and fear a vulnerability. When they see their children using their classroom software, they begin to see and fear a vulnerability.

They haven't forgotten that back in 2015, the Electronic Frontier Foundation filed a complaint with the FTC against Google alleging that their Google for Education platform was exploiting students' personal information and potentially exposing it to third parties. A 2017 report confirmed and expanded on these concerns.

These programs have continued, but Big Tech has left parents with more questions than answers about what is happening with their children's data. How are they pulling in this information? How are they tracking these children? What are they doing with the Chromebook in schools program? Who has this information on their children, and what are they doing with it? What kinds of files are they building about our children?

You know, I have said that one of the questions we should ask and work until we can find an answer is, Who owns the virtual you? Who owns it? Because the virtual you is you and your information online. It is you and your presence online. This is what parents fear.

I will tell you, that fear is complicated because of the rise in mandatory use of technology by students. It has prompted me, along with several of our colleagues here, to ask the FTC to launch a major investigation into how these platforms protect student privacy. That is the question they have to answer. Are you protecting it? If not, why not? If not, are you selling it to the highest bidder? Are you profiting from this educational information?

These security moms know it is not just their kids' safety and privacy at risk. They do their banking online, their shopping online, and they have had to deal with the nightmare of having their identity stolen during one of the many infamous retail hacks.

NATIONAL DEFENSE AUTHORIZATION ACT

Madam President, they also know that these risks aren't just a domestic problem. They have seen bombshell reports about consumer data flowing freely between popular apps and servers in China—of course, China. They have heard about how Chinese companies, all beholden to the Chinese Communist Party—again, as I say so often to American businesses, if you are in business with a company in China, you are in business with the Chinese Communist Party. They know that these companies—all beholden to the Chinese Communist Party—steal intellectual property, build vulnerabilities into their hardware, and tempt tech junkies with flashy mobile apps.

The entanglement doesn't end there. I have spoken on multiple occasions about the clear danger posed by our stifling and overly permissive relationship with China.

We have a duty to address the threats we have uncovered so far and anticipate future problems before they reach our shores. This year's national defense authorization legislation does this by targeting problems in both the public and private sectors.

We know and have known for some time that the agenda of the Chinese Communist Party poses an existential threat to the West. This year's NDAA includes funding and other resources for the Pacific Deterrence Initiative, which is a comprehensive strategy focused on confronting Beijing's influence on other countries and maintaining a U.S. and allied presence in the region. We also authorized a pilot program that will allow cyber specialists from the National Guard to participate in information sharing and analysis between Federal, State, and local officials.

We can use our military and our allies to control a threat that lives half a world away, but how do we stop that threat from reaching our shores?

Back in March, I worked with Senator MENENDEZ to introduce the bipartisan SAM–C Act to secure our pharmaceutical supply chain and protect American consumers from shady Chinese manufacturers. In this year's NDAA, I expanded on that idea and fought for language that will require a percentage of what we call critical technologies to be assembled in the United States or by a close ally.

We are also going to invest even more in machine and advanced manufacturing research at Oak Ridge National Laboratory. Scientists at Oak Ridge will work directly with researchers at the University of Tennessee to develop new technology that will make American companies more competitive.

I will tell you that the University of Tennessee and Oak Ridge Institute are a wonderful partnership. As we work toward 21st-century capabilities for warfare, this is exactly the type of partnership we need to see more of.

Being from Tennessee, which is home to multiple military installations, I know that national defense starts and ends at home, so I secured increased funding that is desperately needed to repair and update Army deployment infrastructure. I know that my friends at Fort Campbell will be able to put that to good use on their runway ramps.

The Defense bill will also fully fund new mission-essential aircraft, including 47 Chinook helicopters for our posts in Tennessee and technologies that will allow those famous Reapers to one day be stationed in the Volunteer State.

We are also finally going to secure some properly fitting body armor for servicewomen, which unbelievably is still unheard of in 2020.

We will likely spend the rest of this week hashing out the finer details of the NDAA before we bring up the final bill for a vote. I encourage my colleagues to consider just how interconnected we are with both our allies and our adversaries. I want them to think about the great power competition and the threats that exist from China, Russia, North Korea, and Iran—I call those four the new axis of evil. I would encourage them to remember that the threats we face require action at every single level, whether they surface at home or half a world away.

I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The senior assistant legislative clerk proceeded to call the roll.

Mr. BOOZMAN. I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. BOOZMAN. Madam President, I rise today in support of the fiscal year 2021 National Defense Authorization Act.

Congress has a constitutional duty under article I, section 8, to provide for the common defense, and the NDAA is one of the key tools that we have to ensure that the United States is capable of defending ourselves and our interests.